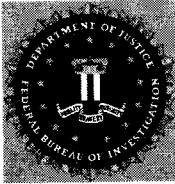


U.S. Department of Justice



Federal Bureau of Investigation

Washington, D.C. 20535

February 27, 2015

MR. ERIK LARSON

Subject: PTECH, INC.
FOIPA Request No.: 1160974-001
Release: 305618

Dear Mr. Larson:

You were previously advised we were consulting with another Government agency concerning information located as a result of your Freedom of Information Acts (FOIA) request.

This consultation is finished and the enclosed material is being released to you with deletions made pursuant to Title 5, United States Code, Section(s) 552/552a as noted below. See the enclosed form for an explanation of these exemptions.

Section 552

☒ (b)(1)

☐ (b)(2)

☐ (b)(3)

☐ (b)(4)

☐ (b)(5)

☒ (b)(6)

☐ (b)(7)(A)

☐ (b)(7)(B)

☒ (b)(7)(C)

☐ (b)(7)(D)

☐ (b)(7)(E)

☐ (b)(7)(F)

☐ (b)(8)

☐ (b)(9)

Section 552a

☐ (d)(5)

☐ (j)(2)

☐ (k)(1)

☐ (k)(2)

☐ (k)(3)

☐ (k)(4)

☐ (k)(5)

☐ (k)(6)

☐ (k)(7)

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), U.S. Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's eFOIA portal at <http://www.justice.gov/oip/efoia-portal.html>. Your appeal must be received by OIP within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Freedom of Information Appeal." Please cite the FOIPA Request Number in any correspondence to us for proper identification of your request.

Sincerely,

A handwritten signature in black ink, appearing to read "D. Hardy", with a stylized flourish at the end.

David M. Hardy
Section Chief,
Record/Information Dissemination Section
Records Management Division

Enclosure

~~SECRET/NOFORN/ORCON~~

b6
b7C

(U) ~~(S/NF/OC)~~ [redacted] is an employee of Ptech Inc., in Boston, and is the [redacted] of Care International, a non-governmental organization in Boston with ties to international terrorism. Care International was previously known as the Al-Kifah Refugee Center of Boston. Following the World Trade Center attack in 1993, Al-Kifah changed its name to Care International after the media reported that members of the Al-Kifah Refugee Center of New York were involved in the attack. In the Boston area, Care International has served as a front for recruiting/funding local Muslims to participate in the international Jihad efforts. [redacted] is closely associated with [redacted] of Care International.

(U) ~~(S)~~ On May 28, 2002, a complainant working for JP Morgan Chase in Manhattan, NY, reported suspicious business practices by Ptech. This complainant was concerned that Ptech was involved in the theft of technology from U.S. companies. This complainant advised that [redacted] is connected to organizations which provide funding for terrorist purposes. This complainant further indicated that a Ptech employee may have tried to gain access to the Chase network during a demonstration of Ptech products and/or services, although there is no independent information to corroborate this.

(U) ~~(S)~~ On August 23, 2002, it was determined that the Information Resources Management (IRM) Office, FBIHQ, had purchased Enterprise Architecture computer software from Ptech in early 2001. This software, named "Framework," was being used as a management tool for the FBI's intranet network and is used for the FBI Enterprise Architecture project. The software allows users to access the FBI's Strategic Plan, organization chart, business processes, and other applications.

(U) ~~(S)~~ Ptech Framework software originals and copies including updated versions and "accelerators" were provided to the Counterintelligence Counterterrorism Computer Intrusion Unit (C3IU), Cyber Division, by IRM for technical analysis. Technical analysis of the Ptech software by the Special Technologies and Applications Section (STAS) to date has not revealed any evidence of malicious (eg. trojans, backdoors, viruses, worms, etc.) or any other unauthorized code imbedded in the software. Examination of two IRM computers used to run the software has not revealed any abnormalities. According to IRM, the Ptech software was not used to connect to the FBI computer network.

(S) ~~(S)~~ [redacted]
[redacted]

~~SECRET/NOFORN/ORCON~~

b1

~~SECRET/NOFORN/ORCON~~

b1

(S)

- (U) ~~(S)~~ IRM personnel (section chief, chief architect, computer scientist, contractors) who worked with the Ptech software on the FBI Enterprise Architecture project have been interviewed. These individuals had no direct contacts or dealings with Ptech or its personnel with the exception of receiving training from instructors from Ptech. The reason is that the Ptech software purchased by the FBI was actually purchased through a government contractor called SPAWAR (Space and Naval Warfare). The interviews did not indicate any unusual or suspicious activity on the part of Ptech or of the performance and operation of the Ptech software used by the FBI.
- (U) ~~(S)~~ C3IU has obtained documents from IRM and the Contracts Unit that relate to the FBI purchase of the Ptech software. The documents indicate that during 12/2001, the FBI purchased two licensed copies of the Ptech Framework software, including updates and accelerators, for use in developing the FBI's Enterprise Architecture (EA) at a cost of \$15,000. The purchase was actually made by SPAWAR on behalf of the FBI and pursuant to the SPAWAR contract.
- (U) ~~(S)~~ The FBI New York Cyber squad has advised that they worked with the security department of JP Morgan Chase Bank, NY, concerning Ptech's efforts to market their software to the bank. JP Morgan security advised that a Ptech representative was allowed limited access to the company's network for this purpose. JP Morgan Chase Bank security conducted a thorough search of all areas of their network accessed by the Ptech representative but did not find any abnormalities. They advised that during a Ptech software demonstration at JP Morgan Bank, JP Morgan denied the Ptech's representative's request to connect his computer with the company's network. As a result of the above dealings with Ptech, JP Morgan did not purchase software from the company.
- (U) ~~(S)~~ Source information and public records have indicated that the Process Renewal Group (PRG) is a consulting group out of Vancouver, British Columbia, Canada. A former Ptech Inc. employee, [REDACTED] was once employed by PRG. Source information has further indicated that PRG never had a contract with the White House as has been claimed by Ptech advertisements and is believed to be fabricated by [REDACTED] and others for the benefit of Ptech. The Contracts Unit, Finance Division, FBIHQ, advised that they failed to locate any records of doing business with PRG.

b6
b7C

~~SECRET/NOFORN/ORCON~~

~~SECRET~~

To: Counterterrorism From: Cyber
(U) Re: ~~(S)~~ 288B-HQ-1394667, 04/04/2003

engaging in activities that pose a threat to U.S. computer networks.

(S) ~~(S)~~

b1

(U) In view of the above, CyD will discontinue any further investigation of the TNII-CT/CI matter, absent any indication of a specific threat posed by Ptech or its products and services to the U.S. information infrastructure. CyD will continue its technical support of the continuing CT investigation concerning individuals associated with Ptech.

~~SECRET~~

~~SECRET/ORDCON/NOFORN~~

To: Counterterrorism From: Cyber Division
Re: ~~(S)~~ 288B-NEW, 08/24/2002

(U)

INTERNATIONAL, a non-governmental organization in Boston with ties to international terrorism and as a source of funding for terrorist activities. [redacted] is the subject of a FBI Boston FFI (199N-BS-86457). [redacted]

b6
b7C

b1

(S) [redacted] This investigation has revealed that CARE INTERNATIONAL serves as a front for recruiting local Muslims to participate in international jihad efforts.

(U)

~~(S)~~ On August 23, 2002, Section Chief Mark Tanner, Information Resources Management (IRM) Office, FBIHQ, advised that the FBI had purchased Enterprise Architecture computer software from Ptech in early 2001. This software, named "Framework," is currently being used as a management tool on the FBI's intranet network and is used for the FBI Enterprise Architecture. The software allows users to access the FBI's Strategic Plan, organization chart, business processes, and other applications.

(U)

~~(S)~~ The Cyber Division is working with the IRM Office to conduct a thorough technical analysis of the Ptech software to determine if the software poses a threat to the FBI network or can be utilized to install a backdoor for later access. The analysis is a two pronged approach. First, an analysis of the software computer compact discs to determine if the software installed any malicious or unauthorized code into the FBI networks, or provides a backdoor to these networks. As of 8/24/2002, preliminary technical analysis of the compact discs conducted by Crucial Security, Special Technology and Applications Unit (STAU), has not revealed any abnormalities. The second phase is to monitor, at the network level, the computer server where the Ptech software currently resides, to look for any anomalous activity of that server with the FBI networks. Crucial Security is currently conducting this type of analysis.

(S)

~~(S)~~ [redacted]
[redacted]
(S) While this analysis of the software and the server's relationship with the FBI network is being conducted, efforts are ongoing to fully identify all government customers of Ptech. Ptech's customers will be advised of the results of the FBI's [redacted] analysis as well as the relationship of Ptech and it's officers with terrorist fund raising activities.

b1

b1

~~SECRET/ORDCON/NOFORN~~

~~SECRET/NOFORN/ORCON~~

backdoors, viruses, worms, etc.) or any other unauthorized code imbedded in the software. Examination of two IRM computers used to run the software has not revealed any abnormalities. According to IRM, the Ptech software was not used to connect to the FBI computer network.

(S)

~~(S)~~

b1

(U)

~~(S)~~ IRM personnel (section chief, chief architect, computer scientist, contractors) who worked with the Ptech software on the FBI Enterprise Architecture project have been interviewed. These individuals had no direct contacts or dealings with Ptech or its personnel with the exception of receiving training from instructors from Ptech. The reason is that the Ptech software purchased by the FBI was actually purchased through a government contractor called SPAWAR (Space and Naval Warfare).

(U)

~~(S)~~ C3IU has obtained documents from IRM and the Contracts Unit that relate to the FBI purchase of the Ptech software. The documents indicate that during 12/2001, the FBI purchased two licensed copies of the Ptech Framework software, including updates and accelerators, for use in developing the FBI's Enterprise Architecture (EA) at a cost of \$15,000. The purchase was actually made by SPAWAR on behalf of the FBI and pursuant to the SPAWAR contract.

(U)

~~(S)~~ The FBI New York Cyber squad has advised that they have been working with the security department of JP Morgan Chase Bank, NY, concerning Ptech's efforts to market their software to the bank. JP Morgan security advised that a Ptech representative was allowed limited access to the company's network for this purpose. JP Morgan Chase Bank security conducted a thorough search of all areas of their network accessed by the Ptech representative but did not find any abnormalities. They advised that during a Ptech software demonstration at JP Morgan Bank, JP Morgan denied the Ptech's representative's request to connect his computer with the company's network. As a result of the above dealings with Ptech, JP Morgan did not purchase software from the company.

~~SECRET/NOFORN/ORCON~~

~~SECRET//NOFORN//ORCON~~

(S)

(S)

[REDACTED]
[REDACTED]
[REDACTED] No positive information was discovered.
[REDACTED]
[REDACTED] No positive information was obtained.
[REDACTED] No positive
information was obtained.

b1

(U)

~~(S)~~ IRM conducted a canvass of all FBI divisions to determine if any other Ptech products were being used or had been acquired. The results of the canvass determined that no one else in the FBI reported acquiring or using any Ptech products. IRM and the FBI has discontinued the use of the Ptech Framework software and a decision has been made not to acquire or use Ptech products in the future.

(S)

~~(S)~~

[REDACTED]
[REDACTED]
[REDACTED] Additional and/or followup interviews of sources, witnesses and former/current employees of Ptech Inc. are also being contemplated when appropriate. The specific purpose of these interviews would be to obtain information concerning Ptech's involvement in planting malicious code or unauthorized code in their software or efforts to implant them in U.S. computer networks.

b1

(U) Investigation continuing.

~~SECRET//NOFORN//ORCON~~

~~SECRET~~

To: Counterterrorism From: Cyber
Re: (S) 288B-HQ-1394667, 10/30/2002

b1

(U) In view of the above, CyD will await the final results of the above Boston, and STAU technical analysis, to assess future investigations needed in connection with captioned investigation and to support the CT investigations.

~~SECRET~~